CLAIMS

1. Method for protecting one or more computer systems using the same secret key (Ks) cryptographic algorithm, characterized in that the way in which said calculation is performed depends, for each computer system and for each secret key, on secret data (Ds) stored in a secret area of the computer system or systems.

2. Protection method according to claim 1, characterized in that, for each computer system and for each secret key (Ks), the way in which said secret data (Ds) is used to perform said cryptographic calculation is public.

3. Protection method according to claim 1, characterized in that there are at least two pieces of said secret data (Ds) used by said computer systems.

4. Protection method according to claim 3, characterized in that each of the computer systems contains at least one specific piece of said secret data (Ds).

5. Protection method according to claim 1, characterized in that in each of the computer systems, there are at least two pieces of said secret data (Ds), corresponding to the various secret keys used by this computer system.

6. Protection method according to claim 5, characterized in that in each of the computer systems, each secret key (Ks) used by said cryptographic calculation corresponds to a specific piece of said secret data (Ds).

7. Method according to claim 1 for protecting one or more computer systems using a cryptographic calculation process using nonlinear transformations of km bits into kn bits described by k conversion tables in which n output bits of the transformation are read at an address that is a function of the km input bits, characterized in that for each of these nonlinear transformations, said k tables are part of the secret data (Ds).

8. Method according to claim 1 for protecting one or more computer systems using a cryptographic calculation process using nonlinear transformations of km bits into kn bits

described by k conversion tables in which n output bits of the transformation are read at an address obtained by applying a secret bijective function (φ) to an m-bit value, itself obtained by applying a public function of the km input bits of the nonlinear transformation, characterized in that for each of these nonlinear transformations, said k tables are part of the secret data (Ds).

9. Protection method according to claim 8, characterized in that for each of the nonlinear transformations, the secret bijective function (φ) is also part of the secret data (Ds).

10. Method according to claim 1 for protecting one or more microcomputer cards, characterized in that the secret data is stored in the E^2PROM memory of said microcomputer card.

11. Protection method according to claim 1, characterized in that a conversion table calculation program is stored in each computer system and activated by a given event in order to calculate the tables and store all or part of these tables in the secret data.

12. Protection method according to claim 11, characterized in that the given event is the exceeding of a given value by a counter.

13. Utilization of the method according to claim 1 to protect a cryptographic calculation process supported by the DES, Triple DES and RSA algorithms.

14. Computer system comprising means for storing a modified cryptographic algorithm that adheres to the computational phases of the standard cryptographic algorithm and uses a secret encryption key contained in a secret area of storage means, and means for executing this modified cryptographic algorithm, characterized in that the computer system comprises first secret means for replacing each intermediate variable required for the computational phases of the standard algorithm with a plurality (k) of partial intermediate variables, second means for applying a nonlinear transformation table to each of these partial intermediate variables, and third secret means for reconstituting the final result corresponding to the utilization of the standard cryptographic algorithm from results obtained on the partial variables.

15. Computer system according to claim 14, characterized in that secret data stored in the secret area includes at least one first random variable v_1 constituting at least one secret partial variable, and the modified algorithm determines at least one other partial variable, for example v_2, by applying a first secret function to the intermediate variable v and the secret partial variable or variables v_1.

16. Computer system according to claim 15, characterized in that the modified algorithm includes means for applying the nonlinear transformations to the partial variables v_1 and v_2 by using tables, at least one of which A, formed by random selection, is stored in the secret data Ds, the other tables required for the calculations being stored in a nonvolatile memory, means for executing the various computational rounds of the standard algorithm, each time using the tables on the partial variables, and means for calculating the result in the last round of the algorithm by combining the partial variables in accordance with a second secret function.

17. Computer system according to claim 14, characterized in that the first secret means of the modified algorithm are constituted by a function *f*, linking the partial intermediate variables and each intermediate variable (v), such that the knowledge of one value of this intermediate variable never makes it possible to deduce all of the particular partial values v_i such that there exists a *(k-1)-tuple* $(v_1, \ldots, v_{i-1}, v_{i+1}, \ldots v_k)$ that satisfies the equation $f(v_1, \ldots, v_i, \ldots, v_k) = v$.

18. Computer system according to claim 14, characterized in that the second means of the modified algorithm are constituted by k partial conversion tables, and among the *k* partial conversion tables, *k-1* partial conversion tables contain secret random variables.

19. Computer system according to claim 18, characterized in that the second means of the modified algorithm comprise k conversion tables, each of these conversion tables receiving as input a value obtained by applying a secret bijective function φ_1 to said function $f(v_1,\ldots, v_k)$ of the partial intermediate variables in accordance with the relation φ_j o $f(v_1, \ldots,v_k)$, $j \in [1,k]$, this application φ_j o $f(v_1,\ldots, v_k)$ being performed by direct evaluation of a resulting value, this resulting value, applied to the input of the conversion table, making

it possible to read *n* output bits of the transformation at an address that is a function of these *m* input bits.

20. Computer system according to claim 14, characterized in that the second means of the modified algorithm comprise means for replacing each nonlinear transformation applied to an intermediate variable of the standard cryptographic calculation process, without a separation, with a partial nonlinear transformation of *km* bits into *kn* bits applied to all of the partial intermediate variables, means for calculating *(k-)n* of said output bits of this transformation as a polynomial function of the *km* input bits, and means for reading the remaining *n* bits of said output bits by reading a conversion table in which the *n* remaining bits are read at an address that is a function of the *km* input bits.

21. Computer system according to claim 14, characterized in that it includes means for sequentially executing the operations performed by the modified algorithm in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

22. Computer system according to claim 14, characterized in that it includes means for executing, in interleaved fashion, the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

23. Computer system according to claim 14, characterized in that it includes means for simultaneously executing the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts, in the event of multiprogramming.

24. Computer system according to claim 14, characterized in that it includes means for simultaneously executing, in different processors working in parallel, the operations performed in the various parts resulting from the separation of the cryptographic calculation process into several distinct calculation process parts.

25. Computer system according to claim 14, characterized in that it includes a conversion table calculation program stored in each computer system and means for the activation by a given event of the calculation of the tables and for the storage of all or part of these tables in the secret data.

26. Computer system according to claim 14, characterized in that a counter includes means for storing a value that is incremented with each cryptographic calculation so as to constitute the given event for the activation, by activating means, of the calculation of the tables when a given value is exceeded.

Add A8>